ОНЛАЙН-ОБРАЗОВАНИЕ

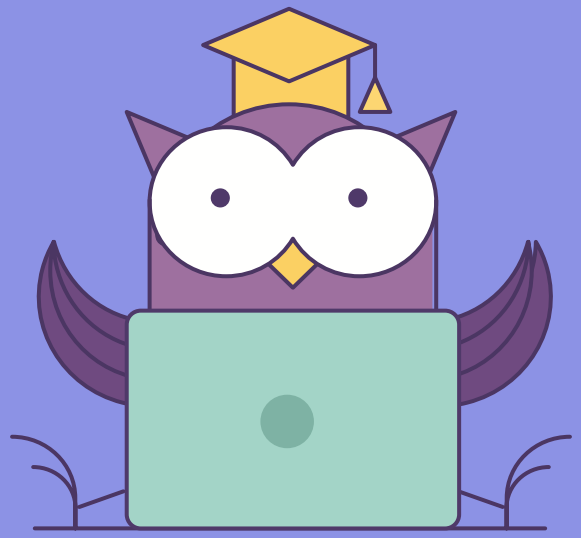
OTUS

Разбор уязвимостей веб-приложений

Часть 4

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Command injection
- Web Cache

- Практика и уязвимости:
  - Web Cache Poison
  - Command Injection

01

Web Cache

Что Такое Web Cache

- Временное хранилище для данных

- **В Web может хранить:**
  - Html страницы
  - Скрипты
  - Медиа

- **Зачем нужно:**
  - Ускорить доступ к данным ресурса
  - Устранить лаги с соединением

- Как и все в Web может быть реализовано как на стороне клиента, так и на стороне сервера

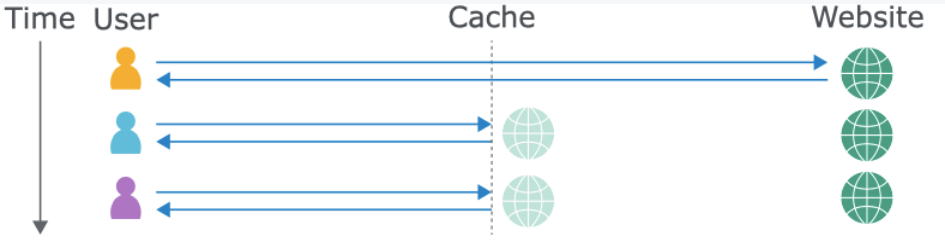
- **Какие продукты популярны:**
  - Varnish
  - HAProxy
  - Squid
  - NGINX
  - Vulcand

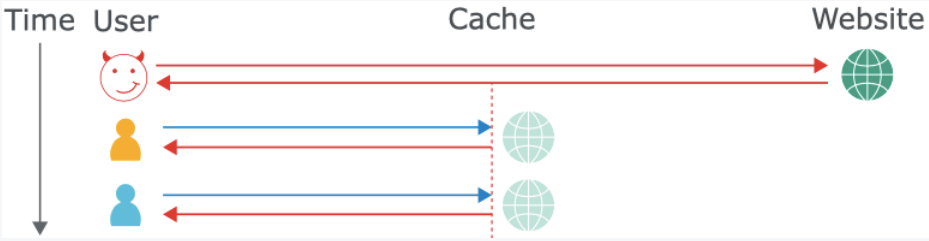
02

WEb Cache poison

Атака web cache poison

- Суть атаки:
  - Выяснить время жизни cache данных
  - Заставить сервер сохранить свои данные
  - Profit
- Что кэшируется:
  - html
  - css,js
  - Media data





03

Command Injection

Command Injection

- Суть атаки:
  - Найти символ
  - Протащить его через WAF
  - Profit
- Где встречается:
  - url
  - Form
  - Любая часть приложения, которая вызывает утилиты через terminal

Тестирование сервисов

Колесников Александр

Спасибо
за внимание!